Accountant Roles Againts Cybercrime in Indonesia Perspective

Made Dudy Satyawan, Rohmawati Kusumaningtias, Susi Handayani

Abstract— The growth of internet usage and website-based applications at this time has grown rapidly almost touching all aspects of the life of the world community. The digital ecosystem roadmap in Indonesia shows that the growth of e-commerce businesses during 2014 to 2018, averaged 17%. Unicorn-based startups such as Go-Jek, Traveloka, Tokopedia, and Bukalapak have valuations above US $ 1 Billion. However, this potential has a negative impact such as increasing cybercrime. The development of cybercrime fosters the responsibility of the accountant profession to develop accounting and audit systems with the aim of detecting, deterring, and preventing the potential for cybercrime within an organization or society. This process will have an impact on the roles, responsibilities, authorities, and obligations of the accounting profession in Indonesia. The introduction of effective policies, procedures and audit tools can help mitigate organizational risk and maximize audit effectiveness. Accountants must also have strong knowledge of information systems and computer technology to carry out ongoing control and supervision and to detect and prevent cybercrime. This article will explore the readiness of the Indonesian accounting profession in facing the threat of cybercrime.

Index Terms— Accountant Roles, Cybercrime, Digital Economy, Indonesia Perspective.

1 Introduction

AT this time where technology is advancing so rapidly, the world of cyber crime is also changing rapidly from the simplest form of identity theft and misuse of the identity theft to take economic advantage of the victim of theft. Today there are more cybercrime evolved than a hacker who stole identity card number or credit / debit card owned by individuals. In fact, the crime of theft of personal data public is just one form of cyber crime world that managed to penetrate the business community today. Others include the takeover of a company account, data theft, and ransomware. Assosiation of International Certified Professional Accountants (AICPA) Information Management and Technology Assurance Cybersecurity Task Force in February 2017 has published a list of cybercrime crimes shown to CPAs in order to enhance their role as trusted independent advisors to give a better protection in corporate organization from data breaches, to keep the information reliable and available when needed.

This article aims to draw attention from the accountants in Indonesia to be able to read the opportunities and challenges of the digital era where technology changes and cyber information is used not only for good, but the sophistication of technology and the Internet in a digital world of cyber security exploited to undermine itself by finding the weakness of the legal system in the country that was attacked by cyber criminals. Pendley (2018) in an editorial review entitled Finance and Accounting Professionals and Cybersecurity Awareness states that it is time for the professional accountant to have the knowledge of various security regulations of privacy in the United States today for the purpose of closing the gap of shortage of security laws computer applicable in the context and specific industry. Finance and accounting professionals can play an important role in protecting information, and to be actively involved in implementation of cyber security. The jurisdiction of Indonesia has Law No. 19 of 2016 on amendments to the Law No. 11 of 2008 on Information and Electronic Transactions which embodies the role of firm government in order to protect the public interest from any kind of disturbances as a result of misuse of Electronic Information and Electronic Transactions.

The Government of Indonesia has also established the Agency Cyber and the State Code (BSSN) of Indonesia which has a scope of work that is focused on the protection of e-commerce, encryption, filtering, cyber diplomacy , cyber crisis management center , centers of information, mitigation support, recovery countermeasures vulnerabilities, incidents and / or cyber-attacks, realizing national security and increasing national economic growth as stated in presidential regulation No. 53 of 2017 as amended by presidential regulation No. 133 of 2017 concerning cyber agencies and state codes.

2 Literature Review

The government does not fend by themselves, for which it takes the crucial role of professional accountants in protecting the economy and the business sector in the digital era as the decision-maker, responsible for risk management, information technology investment decisions and value chain management. Professional accountants need to identify, assess and understand the risks and opportunities of the global information technology trends, so that businesses can grow safely and optimally. So, we need more research that raised the topic of the role of accountants against cybercrime world. Several previous studies that references are from Finau, Samuwai, & Prasad (2013) conducted a study on how information technology changes the way the crime was committed, crime can be done from a distance of millions of miles from the crime scene and have access to big amount of money that could cripple the organization financially.

Cybercrime consists of criminal acts or any behavior which is done through information technologies such as hacking, identity theft, and online fraud. Ngumar (1999) dan Rahmawati (2017) have also been reminded in his research that the impact of the information revolution in the era of globalization has an impact in the disclosure of information,

obscure the structure as well as the traditional boundaries of both sectors of the economy, industry and between countries, thus requiring the role of accountants in Indonesia that ready to face the challenges of globalization by strengthening the mastery of information technology and foreign language skills.

Previous research in line with the results of research conducted by Seetharaman, Patwa, & Niranjan (2017) which states that the auditor also should have a good knowledge of the issues to be audited and the required knowledge of information systems and computer technology to conduct ongoing audits and to detect and prevent fraud computer. For this reason, this article aims to explore any accountant's role towards the prevention and detection of cybercrime as well as the knowledge and skills required to design, develop, monitor system of accounting and auditing (software) -based computer that is effective to prevent and detect the cybercrime.

3 Data and Methods

This study aims to explore secondary data, without operationalizes concept or test the concept of the reality studied using qualitative research methods. Where qualitative research was also considered as a study whose main purpose is to examine the problem or a little understood phenomenon and to develop the initial ideas about it and move toward better research questions Neuman (2014: 38). Cybercrime topics in accounting research are still limited, so explorative research becomes choice for the following reasons: (1) to extend the coverage or expand a phenomenon problem, or a certain behavior, (2) to generate some initial ideas (or "alleged") about the phenomenon, or (3) to test the feasibility of doing extensive studies on the phenomenon. The data sources that is used rely more on literature searches through books, academic literature, working papers from credible institutions, online sources, and other relevant publications.

4 Discussion

Cyber world could not be separated from the massive use of the Internet and digital technologies that drive automation and data exchange in both manufacturing industry, trade and services. Klaus Schwab is the Executive Chairman of the World Economic Forum in his book "The Fourth Industrial Revolution" introduces the term in 2016. Schwab believes, current technology revolution drastically changes the way individuals, corporations, and government work. This fourth-generation industrial revolution characterized by the emergence of a supercomputer, smart robots, vehicles without a driver, cloud computing, big data system, genetic engineering and developmental neuro-technology that allows humans to better optimize brain function. The accounting profession got their challenges and opportunities of the industrial revolution 4.0. Threats can be identified from the interaction of accountants and technologies including the use of robotics and analytics data (big data) takes over the basic work done by accountants (to record the transaction, transaction processing, sorting of transactions). This use is increasing efficiency and effectiveness of the work of the aspects of time to finish the job. Large-scale enterprises have been developing this technology, because it is supported by standardization of the process of financial management and standardize on architecture and information systems.

The utilization of digital technology and its impact on business has changed the accounting practices and competences required by professional accountants. Software and intelligent system (Artificial Intelligence) will replace manual work such as bookkeeping, automate processes (Blockchain) complex and diverse as the completion of the financial statements and accounting reconciliation is not needed anymore. Accountants also need to be aware of the increasing proliferation of cybercrime which has an impact on increasing risk (Cyber Risk) such as the need to create a new control system in the detection, response, and resilience.

Faced with the threat, accountants in the future need to prepare the development about the knowledge of the new model for the business, sources of funding, payments, services, and production will be very important for all professional accountants. Some need to be an expert user of the relevant emerging technologies. Software and intelligent analytic reporting will enable more, better, and closer to real time than today; supporting the transition from a retrospective analysis to prediction; and highlights the linkage of financial performance and non-financial. Video and social media will increase collaboration, disclosures, presentations, and stakeholder engagement (ACCA, 2016). The roles and responsibilities of professional accountants is already far beyond traditional compliance, financial reporting, and their governance role. Over the next decade when the operating environment became sophisticated and complex, professional accountants will move from the head office to the front lines where expertise and experience will be very important to drive economic growth and in enabling businesses to remain resilient and competitive.

Other important point is the role of accountants in anticipation of the rise of cybercrime which could hamper economic growth. Cybercrime is an illegal act involving the use of computers, the Internet or other technologies. Some examples of cybercrime among other actions spread computer viruses (spreading of computer viruses), stalking (stalking), phishing, threats insiders (perpetrating insider threats) and cause a denial of the right of access (denial of service) that when hackers attempt to prevent legitimate users accessing information or services. Criminal activity carried out using media that utilize virtual setting the internet, local network or cloud. Information technology (IT) and the Internet (cyber) has become an integral part of modern human life, starting with the presence of personal computers in offices, internet cafes (cafe), housing and schools. Several major cybercrime facts were revealed that the use of 87 million people of the world account data on Facebook, including 1.1 million accounts from Indonesia affected by the data breach by Cambridge Analytica for the purpose of manipulating the election campaign of America (USA) in 20161. The case in Indonesia in March 2013 involving unscrupulous employees at some stores/merchants care products company Body Shop revealed there has been a crime to use a computer for the purpose of theft of personal data belonging

to buyers making transactions using credit / debit cards Visa International.

The threat of cybercrime has an impact that threaten the confidentiality (confidentiality), integrity (integrity), and availability (availability), and information systems. Accountants in the future should invest more in the development of knowledge and skills in using information technology to help maintain the security of the system and information from the client. The role of accountants is very important in the success of a strategy to increase the security of information technology, since accounting is a "keeper" of financial and information assets is usually the most sought after information by cyber criminals. Finau et al. (2013) stated the importance of developing a forensic accounting profession in the countries of the Pacific, the increasing number of forensic accountants will play an important role in the prevention, detection, and enforcement of cybercrimes. Forensic accountant is a dynamic field and requires knowledge in various subjects such as accounting, law, criminology, and information systems. Massive use of information technology to commit fraud has necessitated the forensic accountant to conversant with information technology and information technology-related crime.

Seetharaman et al. (2017) warns that one of the greatest exposures faced by organizations is a new technology, the auditor should follow the development of information systems and understand the implications of these developments. One significant challenge for auditors is to conduct an examination of the application of new technologies applied to test the organization's control and security issues. Auditor with the skill of computer security should conduct periodic reviews of the system or network security control. The auditor also should have a good knowledge of the subject matter being audited, and the necessary knowledge of information systems and computer technology to conduct continuous audit. The auditors need to understand what is audited and use the appropriate technology to facilitate audits and detect computer fraud.

An important message in the digital world for the accounting profession that is business supposed to consider the issue of cyber in every activity. Businesses also need to adjust the organization's information security system in the era of advanced internet technology and focusing on data protection of critical asset information, because it is impossible for data or information can be protected at the same time. Only the information of the critical data is protected.

5 Conclusion

Accountants have an important role in helping to detect and prevent cyber crime that has the potential to attack an organization or company. Accountants can help identify and reduce the risk of cyber crime in the internal, external, policy making, and protecting the company's reputation. Accountants in order to respond to future developments in information technology is to invest in developing skills in technology as an accountant, increasing knowledge about information technology, being responsive about changes in industry, business, and technological development. In addition, accountants must be able to control financial data security based on technology by integrating conventional financial information into the modern system as is the case in Indonesia today.

References

[1] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet

[2] Davis, J. T. (2012). "Examining perceptions of local law enforcement in the fight against crimes with a cyber component. Policing: An International Journal of Police Strategies & Management, 35(2), 272-284

[3] Directorate of Threat Detection BSSN Indonesia. (2018). Annual report 2018 Honeynet Project BSSN-IHP. Vol 1. ISSN 2655-8467. Jakarta

[4] Finau, G., Samuwai, J., & Prasad, A. (2013). Cyber crime and its implications to the Pacific. The Fiji Accountant, (March), 1–4

[5] Neuman, W. L. (2014). Social Research Methods: Qualitative and Quantitative Approaches. Pearson Education Limited. https://doi.org/10.2307/3211488

[6] Ngumar, S. (1999). Meningkatkan Peran Akuntan. Ekuitas, 3(1), 32–44

[7] Peykanpour, N., & Jalali, F. (2016). Computer Crime, Strategies and the Ways to Deal with them. European Online Journal of Natural and Social Sciences: Proceedings, 5(3 (s)), pp-67

[8] Pendley, J. A. (2018). M ega-disasters : Is Your IT. The Journal of Corporate Accounting & Finance, (January), 53–58. https://doi.org/10.1002/jcaf

[9] Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber. Jurnal Pertahanan Dan Bela Negara, 7(2), 51–66. https://doi.org/10.1016/j.cell.2017.09.020

[10] Seetharaman, A., Patwa, N., & Niranjan, I. (2017). Role of Accountants and Auditors in Mitigating Digital Crimes. Journal of Applied Economics & Business Research, 7(1), 1–17. Retrieved from http://escweb.lib.cbs.dk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=122638701&site=ehost-live&scope=site

[11] Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press

[12] Taylor, R.E., Fritsch, E.J. and Liederbach, J.C. (2014) Digital crime and digital terrorism (3rd edition). Available at: https://www.amazon.com/Digital-Crime-Terrorism3rd/dp/0133458903 (Accessed: 11 August 2016)

[13] The Association of Chartered Certified Accountants. (2016). Professional Accountants-The Future : Drivers of Change and Future Skills. Working Paper

[14] Willison, R., & Warkentin, M. (2012). Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly, 37(1), 1-20